Overview

RiskIQ enables organizations to maintain the integrity of their web and mobile properties by detecting instances of malware, impersonation and defacement used to commit fraud and violate users' privacy. The company's SaaS platform performs continuous asset discovery, indexing and threat detection across websites, mobile app stores and social networks using virtual user technology that emulates human behavior at-scale.

RiskIQ is used by eight of the 10 largest financial institutions in the U.S. and five of the nine leading Internet companies in the world. The company is headquartered in San Francisco and backed by Battery Ventures and Summit Partners.

TECHNOLOGY

RiskIQ created the first and only security platform for web and mobile assets that sees your company's digital assets from the perspective of Internet at-scale. Powered by an extensive crawling infrastructure, our system gathers continuous, real-time data and provides critical analysis to quickly detect threats that both your customers and your brand confront every day.

The RiskIQ discovery and indexing technology creates a dynamic system of record that represents the organization's complete, public-facing digital footprint. RiskIQ enables organizations to understand the scale of its web, mobile and social presence, and take immediate action against domain squatting, defacement, compromised web components, broken links and any other components or properties that pose a threat to prospects, customers and brand.

RiskIQ discovery engine identifies and captures all assets, including assets related to, or claiming to be related to, an enterprise, using basic attributes and identifiers. The discovered assets are indexed and updated continuously, against which business logic, such as security and privacy policies, is applied.

RiskIQ technology is offered as a SaaS solution to realize business and security priorities, including the following capabilities:

- **Discovery:** Identifying all digital assets, including websites, and mobile apps that may lie out of the security organization's direct line of sight.
- **Threat Detection:** Detecting violations of custom-built security, fraud, compliance, and brand use policies.
- **Global Awareness and Analytics:** Providing context and visibility into threats to improve response efficacy.

WEB ASSET MANAGEMENT

The relative ease of attacking, defacing and impersonating web assets has placed a huge burden on enterprises to stay on top of their digital footprint.

RiskIQ is designed to monitor websites and web infrastructure for malicious activity such as defacement, re-directs, and compliance violations. Emulating human online behavior, RiskIQ scans millions of web pages daily to uncover defaced sites, malicious behavior and compliance violations before they do lasting damage.

THREAT INTELLIGENCE FEED

Safeguarding an organization against the potential of attack and understanding motive and intent often requires intelligence data. RiskIQ's Threat Intelligence Feed provides real-time access to data gathered by an extensive proprietary virtual user crawling infrastructure. The knowledge can put to use to defuse current phishing and malware attacks and to develop policies to detect and mitigate future incidents. Subscribers access the full Global Blacklist and multiple threat intelligence feeds.

MOBILE SECURITY

The rapid proliferation of mobile apps and mobile app stores makes it difficult, if not impossible, for organizations to have visibility into and manage all the apps created by their organization, their partners, and malicious apps developed by bad actors.

RiskIQ is designed to provide visibility into the organization's entire mobile ecosystem footprint by identifying and continuously monitoring official apps organizations know about and the rogue apps they don't. By detecting malware, fraud and copycat apps that have the potential to harm organizations and their users, RiskIQ protects organizations' brands across the mobile ecosystem.

- **Detection:** Identify all mobile apps belonging to an organization or claiming affiliation with its brands.
- **Analysis:** Analyze app binaries to detect malicious behavior, risky permissions, and unsafe coding practices.
- **Enforcement:** Automate alerts and remove violations of custom brand use, security, and compliance policies.

BRAND INFRINGEMENT PROTECTION CAPABILITIES

RiskIQ monitors an organization's presence on the Internet at large. By tracking unauthorized web pages, sites and property violations, RiskIQ identifies brand and trademark abuse, domain infringement and phishing targeting organizations and their customers.

- **Detection:** Identify misuse of brand and trademarks in domain names, social media and other web content.
- **Analysis:** Evaluate the nature of brand use in context and determine the level of risk to the organization.
- **Policy Management:** Automate alerts and remove violations of custom brand abuse and security policies.

AFFILIATE OPERATIONS

As organizations and brands expand to include affiliate partners and networks, it becomes increasingly difficult for them to monitor their affiliates for compliance in marketing, pricing and distribution policies.

RiskIQ is designed to give organizations maximum transparency into affiliate operations. With a purpose-built infrastructure, RiskIQ uncovers fraud and violations of corporate and government regulations in affiliate marketing, enabling organizations to take action and reduce their exposure to legal and financial liability.

- **Detection:** Identify fraud and compliance violations in affiliate marketing practices.
- **Analysis:** Provide forensic data through behavioral and reputational analysis.
- **Enforcement:** Automate alerts and remove violations of custom affiliate policies.

www.riskiq.com | info@riskiq.com | +1.888.415.4447